UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/940,985	08/29/2001	Masahiro Kaminaga	NIT-294	5972

7590 10/03/2005

MATTINGLY, STANGER & MALUR, P.C.
Suite 370
1800 Diagonal Road
Alexandria, VA 22314

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 10/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/940,985	KAMINAGA ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) *1-4* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 August 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20010829, 20050808*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election with traverse of Group II, Claims 5-13 in the reply filed on 13 July 2005 is acknowledged. The traversal is on the ground(s) that although the "tamper-resistant processing method of Claim 1 employs a decryption technique using a secret key", the claim is nevertheless directed to a tamper-resistant processing method. This is not found persuasive because the claims of Group I, Claims 1-4, are clearly directed to a public key decryption method using the Chinese Remainder Theorem (CRT). Although the preamble of the claim recites "A tamper-resistant processing method", there is nothing in the body of the claim that would give the phrase "tamper-resistant" patentable weight. The details of the claimed steps only describe steps of a decryption method according to the CRT. The Examiner further notes that Claim 1 requires steps of storing a secret key and inputting a ciphertext, not required in Claims 5, 6, or 11, and that Claim 5, for example, recites steps for transferring an operation unit of data to a register, not required in Claim 1.

The requirement is still deemed proper and is therefore made FINAL.

2. Claims 1-4 are withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected invention, there being no allowable generic or

linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on 13 July 2005.

Drawings

3. Figures 1-4, 20, and 28-30 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 1612, 1614 (see Figure 20); 1807 (see Figure 22); and 2014 (see Figure 25). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application.

5. The drawings are objected to because they include minor informalities. Specifically, in Figure 16, it appears that the second label "BP" denoted by reference numeral 1405 is instead intended to read "BQ", as per the specification at page 36, lines 12-14. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in

reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

6. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, on page 1, line 19, there appears to be text that is not in English. On page 16, lines 2-3, there is a parenthetical note "(refer to "Angouriron Nyuumon")" that appears to be a reference to a document not cited. On page 23, line 3, it appears that "Montgomery's literally work" is intended to read "Montgomery's literary work" or simply

"Montgomery's work". It appears that in the phrase "therefore and it becomes difficult" at page 51, line 14, "and" should be deleted. On page 51, lines 15-16, it appears that the phrase "Although not showing an example" is intended to read "Although an example is not shown". On page 58, line 1, the phrase that the process "will help improve more effect" is generally unclear.

Appropriate correction is required. The above is not to be considered an exhaustive list of errors. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

7. Claims 5-7 and 11 are objected to because of the following informalities: The claims include numerals in parentheses. Numerals in parentheses are reserved for reference characters corresponding to elements recited in the detailed description of the drawings and used in conjunction with the recitation of the same element or group of elements in the claims, so as to avoid confusion with other numbers or characters which may appear in the claims. See MPEP § 608.01(m). Appropriate correction is required.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 5-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al, US Patent 6278783.

In reference to Claims 5, 6, and 7, Kocher discloses tamper-resistant methods including transferring a unit of data A to one register and transferring a corresponding unit of data B to a second register, where the order of transfer to the registers is determined by a random number. Kocher further discloses executing an arithmetic operation on the contents of the registers, storing the result, and repeating the above steps until the operation has been completed (see column 6, lines 39-63; column 9, lines 1-23; column 10, lines 16-38 and 51-60).

In reference to Claims 8, 9, and 10, Kocher further discloses that the arithmetic operation can be sum, product, XOR, AND or OR (see, for example, column 2, lines 44-45).

10. Claims 11-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Jahnich et al, US Patent 6725374.

In reference to Claims 11 and 12, Jahnich discloses a tamper-resistant processing method including selecting an unprocessed operation unit in data A corresponding to a generated random number, executing an arithmetic operation on the unit of the data A and a corresponding unit of data B, storing the result, and repeating the above steps until the operation has been completed (column 5, line 51-column 6, line 24; see also column 5, lines 25-35). In reference to Claim 13, it is well known that logical OR, AND, and XOR are operations performed in computer processes.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kocher et al, US Patent 6327661, discloses a system for preventing information leakage from smart cards including random permutations of values in registers.

b. Ryan, Jr. et al, US Patent 6748535, discloses a system and method for preventing differential power attacks on a smart card.

c. Akkar et al, US Patent Application Publication 2001/0012360, discloses a method for avoiding differential power analysis in smart cards including random permutation of operations.

d. Messerges et al, "Investigations of Power Analysis Attacks on Smartcards", discusses the need to defend cryptographic methods from power analysis attacks when cryptanalyzing and protecting an encryption algorithm.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

340
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER